CLAIMS

We claim:

1. A method for providing secure access to information held in a shared repository, comprising the steps of:

storing, on a data server, information provided by a data owner;

providing, to the data owner, a data owner public key and a data owner private key, the data owner public key and the data owner private key being a first key pair of a public-key cryptography system;

providing the data owner public key to the data server;

providing, to a data user, a data user public key and a data user private key, the data user public key and the data user private key being a second key pair of the public-key cryptography system;

providing the data user public key to the data server;

sending the data user public key from the data user to the data owner;

encrypting the data user public key by the data owner, using the data owner private key, to provide an encrypted data user public key;

sending, by the data owner to the data server, the encrypted data user public key and a command that gives the data server permission to transfer the information to the data user;

decrypting the encrypted data user public key, using the data owner public key, to provide a check word;

comparing the check word and the data user public key; and

if the step of comparing the check word and the data user public key indicates that the check word and the data user public key match, recording permission to transfer the information in an access list.

2. The method of claim 1, further comprising the steps of:

receiving, by the data server, a request by the data user to transfer the information to the data user;

responsive to receiving the request, checking the access list to determine whether the data server has permission to transfer the information;

if the data server has permission, encrypting the information using the data user public key to provide encrypted information; and

transferring the encrypted information to the data user.

3. The method of claim 1, further comprising the steps of:

encrypting the data owner public key, by the data user, using the data user private key, to provide an encrypted data owner public key;

sending, from the data user to the data server, the encrypted data owner public key and a request to transfer the information to the data user;

decrypting the encrypted data owner public key using the data user public key, to provide a second check word;

comparing the second check word and the data owner public key;

if the step of comparing the second check word and the data owner public key indicates that the second check word and the data owner public key match, checking the access list to determine whether the data server has permission to transfer the information; and,

if the data server has permission, transferring the information from the data server to the data user.

4. The method of claim 3, further comprising the step of sending the data owner public key from the data owner to the data user.

5. The method of claim 1, wherein the information includes an electronic business card.

6. A method for providing secure access to information held in a shared repository, comprising the steps of:

storing, on a data server, information provided by a data owner;

providing, to the data owner, a data owner public key and a data owner private key, the data owner public key and the data owner private key being a first key pair of a public-key cryptography system;

providing the data owner public key to the data server;

providing, to a data user, a data user public key and a data user private key, the data user public key and the data user private key being a second key pair of the public-key cryptography system;

providing the data user public key to the data server;

sending the data user public key from the data user to the data owner;

combining, by the data owner, the data user public key and a sequence number, to provide a combination;

encrypting the combination by the data owner, using the data owner private key, to provide an encrypted combination;

sending, by the data owner to the data server, the encrypted combination and a command that gives the data server permission to transfer the information to the data user;

decrypting the encrypted combination, using the data owner public key, to provide a decrypted combination;

parsing the decrypted combination to provide a check word and a check number;

comparing the check word and the data user public key;

comparing the check number and an expected sequence number; and

if the step of comparing the check word and the data user public key indicates that the check word and the data user public key match, and further if the step of comparing the check number and an expected sequence number indicates that the check number and the expected sequence number match, recording permission to transfer the information in an access list.

7. The method of claim 6, further comprising the steps of:

receiving, by the data server, a request by the data user to transfer the information to the data user;

responsive to receiving the request, checking the access list to determine whether the data server has permission to transfer the information; and,

if the data server has permission, encrypting the information using the data user public key to provide encrypted information; and

transferring the encrypted information to the data user.

8. The method of claim 6, further comprising the steps of:

encrypting the data owner public key, by the data user, using the data user private key, to provide an encrypted data owner public key;

sending, from the data user to the data server, the encrypted data owner public key and a request to transfer the information to the data user;

decrypting the encrypted data owner public key, using the data user public key, to provide a second check word;

comparing the second check word and the data owner public key;

if the step of comparing the second check word and the data owner public key indicates that the second check word and the data owner public key match, checking the access list to determine whether the data server has permission to transfer the information; and,

if the data server has permission, transferring the information from the data server to the data user.

9. The method of claim 8, further comprising the step of sending the data owner public key from the data owner to the data user.

10. The method of claim 6, wherein the information includes an electronic business card.